Masterminding change by combining secure system design with security risk assessment

Florian Kammüller, Axel Legay, Stefano Schivo

Middlesex University London and Technische Universität Berlin, Germany
Université Catholique du Louvain, Belgium
Open University, the Netherlands
f.kammueller@mdx.ac.uk, axel.legay@uclouvain.be, stefano.schivo@ou.nl

Abstract. This track introduction presents the results of the Workshop on Security practices for Internet of Things, SPIoT held at ETAPS in Prague in April 2019. For this Special Issue of STTT, we have selected, invited and edited three distinguished papers. We briefly recall the aims, summarize the Workshop held in Prague and introduce the selected papers.

Secure systems are a moving target in the literal sense since they are targeted by attackers but also for system engineers: they need development methods that allow for dynamic change to make up for continuously arising new vulnerabilities of systems previously believed (and maybe even proved) to be secure.

System models need to be concise which is achieved by omission of details; refinement into concrete systems adds details not present in the abstract model. Systems may be proved to be secure on the abstract specification and yet attacks may arise that exploit details added by those refinements. In short, attacks unforeseen by security proved system specifications come from outside the model.

A real challenge worthwhile to be master-minded is to build a dynamic development process that pre-meditates unforeseen vulnerabilities. Such a process must integrate good engineering practice of co-designing the system together with the attacker's possibilities: a process that interleaves secure system design methods with security risk assessment methods.

Established industry-strength methods for secure system design as well as security risk assessment exist: for example formal system specification, quantitative model checking and attack tree analysis. Distributed systems based on the Internet of Things (IoT) seem to allow building more flexible human centered systems. However, a malicious attacker can easily exploit IoT devices to build botnets, lock them with ransomware, or use them as a bridgehead into less accessible networks.

This STTT Special Issue focuses on presenting a few competitive industrial strength approaches on building holistic yet dynamic secure systems that mastermind the challenges posed by supporting the formal process for developing secure IoT systems.

The objective of the SPIoT workshop has been to bring together security practitioners, security-aware IoT users and formal analysis experts with the aim

of sharing practices and finding guarantees about the trustworthiness of IoT devices and their use. Relevant case studies came from settings where a security flaw implies serious damage, such as in industry, safety-critical systems and healthcare.

Besides presentations of the selected papers below, Jan Kretinsky from TU Munch presented an invited talk on *Expected Cost Analysis of Attack-Defence Trees*.

One of the workshop organizers, Florian Kammüller, presented *Security Engineering in Isabelle* [4] summarizing some of the key findings of the CHIST-ERA project SUCCESS [7] addressing Security and Privacy in the IoT for healthcare applications. In this talk, Kammüller showed how to derive formal specifications of secure IoT systems by a process that uses the risk assessment strategy of attack trees on infrastructure models. The models of the infrastructure are logical models in the Isabelle Infrastructure framework [4]. It comprises actors, policies and a state transition of the dynamic evolution of the system. This logical framework also provides attack trees [2]. The process he proposed in this talk incrementally uses those two features to refine a system specification until expected security and privacy properties can be proved. Infrastructures allow modeling logical as well as physical elements which makes them well suited for IoT applications. Kammüller illustrates the stepwise application of the proposed process in the Isabelle Insider framework on the case study of an IoT healthcare system of the SUCCESS project context [3].

A project partner of the SUCCESS project and another co-organizer of the Workshop, Marielle Stoelinga, presented a visionary talk on *Learning from attacks and failures: generating reliability models from data*. In this talk she summarized the lessons learned from previous work [5] on integrating fault tree analysis with attack trees for quantitative analysis. She sketched the research landscape and future challenges for formal methods in the presence of machine learning that are partly addressed in her current work on rare-event simulation [1].

The other papers presented at the ETAPS Workshop SPIoT on 7. April 2019 in Prague that are published in this Special Issue are briefly introduced below. They were selected and peer-reviewed after the workshop.

- *Static Analysis for Discovering IoT Vulnerabilities* (by Pietro Ferrara, Amit Mandal, Agostino Cortesi, and Fausto Spoto).
  The OWASP Top 10 Internet of Things 2018 is a list of security vulnerabilities for IoT systems. In this paper, the authors discuss the relationship between these vulnerabilities and the ones listed by OWASP Top 10 (focused on Web applications) and how these vulnerabilities can be exploited as well as how static analysis may prevent them. Furthermore, it is demonstrated how the industrial analyzer Julia covers a large portion of the OWASP Top 10 vulnerabilities.
- *ADTLang: A Programming Language Approach to Attack Defense Trees* (by René Rydhof Hansen, Peter Gjøl Jensen, Kim Larsen, Axel Legay, and Danny Bøgsted Poulsen)

This paper presents an extension of Attack Defense Trees by temporal dependencies between attacks leading to a specific ordering for successful attacks and policies for the defender. Moreover, the authors introduce a Domain Specific Language (DSL) and an accompanying tool based on well-established tools for formal methods to produce the given results with non-trivial and automatic translation to and from the target formalisms. The usefulness of the framework is exhibited on a small running example using the policy notion to implement a reactive Break The Glass policy.

– *Graph-based Technique for Survivability Assessment and Optimization of IoT Applications* (by Vladimir Shakhov and Insoo Koo.)
To make IoT solution more robust against failure or being hacked into, the authors propose using quantitative methods to provide a means for considering the trade off between IoT resources and system survivability. The approach combines specificity of network topology, intrusion details, and properties of intrusion detection/prevention system. This work combines graph theory and stochastic process-based models describing the network topology as a probabilistic graph. An approach for deduction and computation of this survivability metric is discussed. Survivability optimization problems are formulated. In some important practical cases closed-form solutions are offered.

References

1. C. E. Budde, M. Biagi, R. E. Monti, P. R. D'Argenio and M. Stoelinga, Rare event simulation for non-Markovian repairable fault trees, *26th International Conference on Tools and Algorithms for the Construction and Analysis of Systems, TACAS 2020*, LNCS, Springer, 2020.
2. F. Kammüller, Attack Trees in Isabelle, *20th International Conference on Information and Communications Security*, LNCS **11149**, Springer, 2018.
3. F. Kammüller, Combining Secure System Design with Risk Assessment for IoT Healthcare Systems, *Workshop of Security, Privacy, and Trust in the IoT, SPTIoT'19, colocated with IEEE PerCom'19*, https://doi.org/10.1109/PERCOMW.2019.8730776, IEEE 2019.
4. F. Kammüller. A formal development cycle for Security Engineering in Isabelle, 2020. http://arxiv.org/abs/2001.08983arXiv:2001.08983.
5. E. Ruijters, D. Reijsbergen, P.-T. de Boer, N. Stoelinga, Rare Event Simulation for Dynamic Fault Trees, *Computer Safety, Reliability, and Security*, Springer, Cham, pp. 20–35, 2017.
6. Workshop on Security practices for Internet of Things, co-located with *European Joint Conferences on Theory and Practice of Software, ETAPS'19*, https://conf.researchr.org/track/etaps-2019/spiot-2019-papers Sat 6 – Thu 11 April 2019 Prague, Czech Republic.
7. CHIST-ERA. Success: Secure accessibility for the internet of things, 2016. http://www.chistera.eu/projects/success and https://github.com/success-iot.